ABSTRACT

The present invention makes it difficult for unauthorized parties to estimate processing and a secret key based upon the waveforms of power consumption of an IC card chip by changing a processing order in the IC card chip so that it is not estimated by the attackers. In an information processing apparatus comprising storing means having a program storing part for storing programs and a data storing part for storing data, an operation processing unit, means for inputting data to be operated on in the operation processing unit, and means for outputting operation processing results on the data by the operation processing unit, an arithmetic operation method is provided which comprises the steps of: for two integers K1 and K2, when finding a value F(K, A) of a function F satisfying F(K1+K2, A)=F(K1, A)○F(K2, A) (○ denotes an arithmetic operation in a communtative semigroup S. K designates an integer and A designates an element of S), decomposing the K to the sum of m integers K[0] + K[1] + … K[m-1]; using T(0), T(1), … T(m-1) resulting from rearranging a string of the m integers 0, 1, … m-1 by permutation T (the result corresponds one for one to the integer string 0, 1, … m-1); and operating on terms F(K[T(0)], A) to F(K[T(m-1)], A) on the right side of

$$F(K,\ A) = F(K[T(0)],\ A) \bigcirc F(K[T(1)],\ A) \bigcirc \ \ldots F(K[T(m-1)],\ A)\ \ldots\ \text{(expression 1)}$$

in the order of F(K[T(0)], A), F(K[T(1)], A), … F(K[T(m-1)], A) to find F(K, A).